Written Testimony of

Mark Schneiderman, Senior Director of Education Policy
Software & Information Industry Association (SIIA)

To
Virginia Joint Commission on Technology and Science

Hearing On
Cloud Computing & Student Data

August 6, 2014
Richmond, Virginia

On behalf of the Software & Information Industry Association (SIIA) and our member high-tech companies, thank you for hearing my testimony today on Senate Bill No. 599, cloud computing and student data. I am Mark Schneiderman, SIIA's senior director of education policy. SIIA agrees with the need to safeguard student privacy and security. A strong network of laws and business practices now does so. SIIA is concerned that Senate Bill 599 may inappropriately and unnecessarily inhibit core educational functions necessary to serve Virginia's students.

As background, SIIA is the principal trade association for the software and digital content industry. Many SIIA members work with schools and universities in Virginia and nationwide to develop and deliver learning software applications, digital content, web services and related technologies. Many of these services involve the use of student information. They are helping to support teachers and instruction, improve student learning, carry out various administrative operations, and improve school productivity and educational performance. SIIA and our members agree with the priority of safeguarding student privacy and data security.

Educational Benefits of Technology & Data

The use of student information in schools is nothing new. From school bus scheduling to supporting teachers to adaptive learning software, our schools have a long history of effectively using information, and of relying on technologies from school service providers.

Today, new technologies like cloud computing and data analytics are enhancing school capacity, increasing teacher access, improving security, and improving functionality. It is important to understand that cloud computing and similar technologies keep the data access and authorization controls in the hands of schools. Like a safety deposit box in a bank, the owner – in this case, the school – determines what is maintained in the box, how that valuable is used, and who has access.

The result of these tools is the ability for school systems to better identify students at risk of failure, to better identify the lessons that best meet each student's unique needs, and to carry out core school administration. These tools and techniques allow educators to manage more data in more cost effective and sophisticated ways to inform instruction and enhance school productivity

As such, technology and data systems are increasingly mission critical to supporting students, families and educators – providing operational efficiencies, informing practice, and helping address the unique learning needs of each student. Modernizing our educational system through technology is critical to delivering a world-class education to all students, and ensuring the nation's international competiveness.

Student Privacy & Security Protections

Schools and service providers have a strong framework of policies and procedures in place to safeguard the privacy and security of student information. One way they do this is by limiting the use of student personal information to legitimate educational purposes.

The federal Family Educational Rights and Privacy Act (FERPA) requires that:

- student personally identifiable information shared with service providers be limited to uses otherwise performed by the school's own employees,
- the provider and information be under direct control of the school, and
- the information can only be used for educational purposes.

In addition, the federal Children's Online Privacy Protection Act (COPPA) requires consent for child-directed online and mobile collectors of personal information, including related to behavioral advertising, from children under 13, both inside and outside of schools. The school may provide consent only where the collection is for the use and benefit of the school and not for other commercial purposes, and the operator must provide the school with full notice of its collection, use, and disclosure practices.

COPPA and FERPA require parental consent both
(1) if the school wants to share personal student information for non-educational purposes; and
(2) if the operator wants to use or disclose the information for its own commercial purposes.

The Protection of Pupil Rights Amendment (PPRA) prohibits use of personal information collected from students for marketing and advertising purposes unrelated to the educational purpose for which it was collected.

Service providers are also bound by contract, privacy policies and their terms of service agreements, and they are subject to significant penalties for unauthorized disclosure of personal student information. There is also a market incentive for service providers: if they do not live up to their responsibilities, they will lose the confidence of their customers.

Senate Bill 599

SIIA is concerned that Senate Bill 599 may inappropriately and unnecessarily inhibit core educational functions necessary to serve Virginia's students. SIIA has several concerns.

First, the bill's definition of "student data" is inconsistent with generally accepted fair information practices and the federal FERPA law. Specifically, the bill's definition would seem to include any and all data "about a student" whether or not the information is personal or personally identifiable. School districts and their service providers use de-identified, aggregate, and other anonymous information for

many purposes critical to the delivery and improvement of educational services, but its use does not raise privacy concerns.

Second, SIIA is concerned with this provision that "No cloud computing service provider shall use *cloud computing services* for any secondary purpose . . ." By definition, cloud computing technology infrastructure is often used to serve a variety of uses and users, but that shared computing does not mean the data is shared. As such, the legislation would seem to violate basic property ownership rights by restricting the cloud computing service provider's use of their own computer hardware and software.

Third, SIIA is concerned with the unlimited scope of the restriction that "No cloud computing service provider shall use cloud computing services *for any secondary purpose that benefits the service provider* or a third party, . . ." SIIA is concerned the effect of 599 would be to block appropriate use of student data for educational purposes that would benefit students and a local school board such as to improve the very educational services in question. It is unclear where the line would be drawn between primary and secondary purposes.

Fourth, the bill would take control away from local educators, school boards, and parents. The blanket prohibitions for uses of student information would trump the long standing framework giving parents opportunity to consent to additional data uses should they desire.

Finally, the one-size prohibitions on building a profile, behavioral advertising and secondary uses ignore that the educational version of such activities may in fact be desired and necessary as core to delivery of the very educational service that educators and parents are seeking, including simply signing in to use applications and other internal operations, adaptive learning software, and uploading student created content.

Student Privacy Policy Guidelines

SIIA and our member companies agree with the need to review and improve public policies as needed. However, we are concerned some of the policy solutions may be ahead of and over-correct the actualized problems. We want to ensure that well-intentioned policies intending to create a floor of student privacy protections do not instead create a digital learning ceiling.

Several months ago, SIIA released "Policy Guidelines for Building a Student Privacy Trust Framework" (http://bit.ly/SIIAStudentPrivacyPolicyGuidelines). SIIA encourages policymakers to:

- provide local communities and school officials with sufficient flexibility, and avoid policies that are overly restrictive or make impractical requirements as these could have a chilling effect on schools and service providers and stifle educational improvement;
- ensure new legislation is consistent with the substantial protections in existing federal regulations to avoid conflict and confusion; and
- limit the scope to student personally identifiable information.

SIIA suggests the following best approaches for policy:

- Educate, equip, and empower schools and educators to make informed decisions that safeguard student data and serve student learning.
- Encourage transparency by schools and school service providers.
- Put in place state and district level governance bodies with oversight for determining specific student data policies and practices.
- Build capacity, including professional development, technology tools for managing and securing that data, and student digital literacy.

- Identify what issues Virginia districts must address, and give them flexibility in how those are addressed.

SIIA agrees student personal information:

- should not be used for non-educational purposes; and
- should be used only for the educational purposes for which it was entrusted (authorized and directed).

Usage policy should give educational agencies the flexibility to best meet their needs and determine which data to collect, with whom to share it, and for what educational and school purposes.

Public policy should not conflate "commercial use" with the appropriateness of a use simply because the service provider is for-profit. Policies should not inhibit service providers from using student information for educational uses authorized by its users, such as:

- for providing the service including through subcontractors
- for educational product evaluation, improvement, and development
- to drive adaptive and customized learning.

Student information should not be sold to insurance companies or used to target insurance advertising, for example. At the same time, polices should enable new models that expose students, teachers, and families to learning opportunities that "work with students like you." So long as student personally identifiable information is not shared with unapproved entities, restrictions around "marketing" or "advertising" for non-educational purposes should not be confused with recommendations about the next appropriate module.

Let me conclude by highlighting that much has happened since the Virginia legislature last considered these bills:

- industry and educators are further articulating best practices, and providing related training;
- educational agencies are further reviewing data applications and putting in place supplemental agreements with service providers;
- government agencies are updating regulations and guidance; and
- school service providers are clarifying privacy policies and other terms to clarify the safeguarding of student privacy.

SIIA agrees with the need to safeguard student privacy and data security. SIIA encourages the reliance on this existing law and on empowering local schools to determine what is or is not appropriate within the already restrictive federal regulations. SIIA urges that any further government regulations be carefully crafted so that efforts to create a privacy floor do not unintentionally limit educational services and benefits, and reduce educational opportunities for Virginia students.

I would be happy to answer any questions you might have.